REMARKS

The application has been reviewed in light of the Office Action dated November 10, 2004. Claims 1-18 are pending in this application, with claims 1-2, 7-12 and 17-18 being in independent form. It is submitted that no new matter has been added and no new issues have been raised by the present Amendment.

Figures 2 and 3 were objected to by the Examiner. Applicant has corrected the drawings in the manner suggested by the Examiner. Withdrawal of the objection to the drawings is respectfully requested.

Claims 1-18 were rejected under 35 U.S.C. §102(e), as allegedly anticipated by U.S. Patent No. 6,357,008 to Nachenberg. Applicants have carefully considered the Examiner's comments and the cited art, and respectfully submit independent claims 1-2, 7-12 and 17-18 are patentably distinct from the cited art, for at least the following reasons.

Independent claim 1 relates to a method for detecting decryption of encrypted viral code in a subject file, comprising, emulating computer executable code in a subject file, flagging a memory area that is read during emulation of a first instruction in the computer executable code, and detecting a modification to the flagged memory area during emulation of a second instruction in the computer executable code.

Nachenberg, as understood by the Applicant, relates to a method for detecting computer viruses using decryption, exploration and evaluation phases. The decryption module of Nachenberg "determines whether or not the just-emulated instruction modifies the content storead at a (virtual) memory address . . . ." (Nachenberg, column 9, lines 5-9). If a modification is performed by the just-emulated instruction, then the decryption module records the modification (Nachenberg, column 9, lines 11-16). In other words, the method described in Nachenberg simply emulates an instruction and immediately records any

modification to that same instruction.

However, Nachenberg is not understood to teach or suggest a method for detecting decryption of encrypted viral code in a subject file, comprising, emulating computer executable code in a subject file, flagging a memory area that is read during emulation of a first instruction in the computer executable code, and detecting a modification to the flagged memory area during emulation of a second instruction in the computer executable code, as recited in independent claim 1.

Accordingly, Applicant submits independent claim 1 is patentably distinct from the cited art. Independent claims 7, 9, 11 and 17 are believed to be patentably distinct from the cited art, for at least similar reasons.

Applicant also finds no teaching or suggestion in the cited art of a method of detecting encrypted viral code in a subject file, comprising emulating computer executable code in a subject file, maintaining a list of memory regions that have been read and then modified during the emulation, determining whether a memory area is read during emulation of a first instruction in the computer executable code and whether the memory area is modified during emulation of a second instruction in the computer executable code, updating the list of memory regions to include the modified memory area and triggering a viral detection alarm, if one of the listed memory regions is larger than a predetermined size, as recited in independent claim 2.

Accordingly, Applicant submits independent claim 2 is patentably distinct from the cited art. Independent claims 8, 10, 12 and 18 are believed to be patentably distinct from the cited art for at least similar reasons.

The Office is hereby authorized to charge any additional fees that may be required in connection with this amendment and to credit any overpayment to our Deposit Account No. 03-3125.

If a petition for an extension of time is required to make this response timely, this paper should be considered to be such a petition, and the Commissioner is authorized to charge the requisite fees to our Deposit Account No. 03-3125.

If a telephone interview could advance the prosecution of this application, the Examiner is respectfully requested to call the undersigned attorney.

Entry of this amendment and allowance of this application are respectfully requested.

Respectfully submitted,

RICHARD F. JAWORSKI
Reg. No.33,515
Attorney for Applicants
Cooper & Dunham LLP
Tel.: (212) 278-0400